IAB Europe's Position on the

Draft Digital Omnibus on the Digital Acquis

IAB Europe has a diverse membership that comprises a variety of digital marketing, digital advertising and media companies. IAB Europe welcomes the European Commission's ambition to simplify the EU digital acquis, reduce unnecessary regulatory burdens, and address consent fatigue, while maintaining a high level of data protection.

We appreciate the opportunity to share recommendations on how the draft regulation can be clarified to better deliver simplification, legal certainty, and workable outcomes for the digital advertising ecosystem and the wider European digital economy.

This document focuses on GDPR related provisions of the Digital Omnibus proposal, including Articles 4, 9, 35, 41a, 88a and 88b.

A note, which elaborates on the challenges posed by Article 88b, is also annexed to this paper.

Executive summary and key recommendations

The European Commission's ambition to streamline the EU digital acquis and promote a more harmonised, risk-based application of the GDPR is strongly welcomed. Measures such as harmonising the implementation of Data Protection Impact Assessments and introducing a single entry point for data breach notifications have the potential to reduce compliance burdens and address regulatory fragmentation across Europe. This approach, which favours simpler and risk-based rules, should guide the work of the co-legislators throughout the legislative process.

At a high level, we recommend:

- **The co-legislators should support the underlying objective of the amended definition of personal data, which is crucial for greater legal certainty.** This change, which aims to align the GDPR definition with the CJEU's ruling in EDPS v SRB, will incentivise the responsible use of pseudonymisation and anonymisation techniques that can meaningfully reduce or prevent the ability to (re-)identify

individuals in practice (Article 4). To facilitate a more realistic evaluation of identification risk, Recital 27, which relates to this, requires further clarification.

- **The co-legislators should back the Commission's proposal to use secondary legislation to delineate the boundaries of the GDPR more clearly.** IAB Europe considers an implementing act the most effective tool to ensure a more consistent interpretation of the revised definition of personal data across the EU (Article 41a). The co-legislators should also broaden the scope of this new article to explicitly cover anonymisation, in addition to pseudonymisation.

- **The co-legislators should explicitly recognise privacy-enhancing technologies as technical safeguards against the re-identification of pseudonymised data**. While technical measures are essential, the Commission proposal should be amended to better reflect the role of organisational and contractual measures in preventing (re-)identification (Article 41a).

- **The most effective route to genuine simplification is to repeal the ePrivacy cookie rule entirely and rely solely on the GDPR**. Retaining ePD Article 5(3) for non-personal data risks establishing a stricter regime for accessing information that cannot even be linked to an identifiable individual. Meanwhile, Article 88(a) departs from the GDPR's risk-based framework by mandating consent as the default legal basis for processing of personal data originally accessed on devices - an approach that will not address the issue of consent fatigue. Although establishing clear consent exemptions is positive, the proposed list should be broadened to encompass a wider range of essential, low-impact use cases, consistent with a risk-based approach (Article 88a).

- **The draft legislation should not impose a rigid consent renewal timeline, acknowledging the diversity of processing activities, online services and technical environments**. Mandating a six-month consent renewal would be technically unworkable across different online environments and poses a threat to the economic viability of media (Article 88a (4)).

- **The co-legislators should abandon the introduction of centralised consent tools**. The latter revives a repeatedly abandoned concept that is legally flawed, technically unworkable, and economically harmful. Instead, the co-legislators should address the root cause of banner proliferation: the excessive reliance on consent as the legal base for all but a few cookie uses without regard to actual risk of harm (Article 88b).

- **While the goal of protecting media publishers is welcome, the proposed exemption - allowing media service providers to ignore browser-level signals -**

does not fully achieve this. As drafted, it risks undermining the advertising-based business models most media publishers rely on, falling short of simplification and legal certainty (Article 88b(3)).

Observations and recommendations on key issues

1. Access and storage of personal data in the terminal equipment and subsequent processing (GDPR article 88a - paragraphs 1, 2, 3 and 5 - and ePD article 5(3)).

While the intention behind the revised cookie rules is positive, the current draft does not deliver meaningful simplification or address consent fatigue. A central promise of the draft regulation was to reduce unnecessary regulatory friction, improve user experience, consider a risk-based approach for access and storage and enhance the competitiveness of European digital businesses. However, the proposals on 'cookies' do not deliver on this ambition. The draft legislation cements consent as the default legal base for all data storage and access techniques, including a wide range of low-impact activities, continuing to impose significant operational burdens without commensurate privacy benefits. This will not reduce the number of consent requests consumers encounter, therefore perpetuating consent fatigue. In addition, the proposal creates a dual regime for personal vs. non-personal data (see GDPR article 88a vs. ePD article 5(3)), resulting in a stricter framework for the processing of non-personal data than for personal data. This fragmentation will create uncertainty as to which regime applies to whom and when, and increase not only implementation complexity but also user confusion.

Repealing the ePrivacy cookie rule and relying fully on the GDPR is the most effective path to genuine simplification. If the stated objective of the Commission proposal is to consolidate overlapping requirements between the ePrivacy Directive and the GDPR, the most effective and legally coherent solution would be to repeal the cookie-related provisions of the ePrivacy Directive (i.e. ePD article 5(3)), given that all processing of personal data collected through cookies is already subject to the GDPR's comprehensive and risk-based framework, while unauthorised access to devices remains strictly prohibited under existing national computer misuse law (cybercrime directive 2013/40/EU). This would allow essential, low-impact activities to proceed under an alternative legal basis such as legitimate interest, subject to the GDPR's robust balancing test and safeguards. When these processing activities do not meet the GDPR's conditions for reliance on an alternative legal base, such as legitimate interests or contract, they would continue to be governed by consent requirements.

Establishing clear consent exemptions can be valuable to improve legal certainty but the proposed list needs clarification to be effective in digital supply chains. In particular, the exemption for first-party analytics (see article 88a (3b)) is drafted too narrowly, limiting it to processing carried out solely by the controller of the service and exclusively for its own use. This interpretation is more restrictive than existing national regulatory guidance, which recognises that analytics are often performed by specialist third-party processors or controllers on behalf of publishers - and other service providers - and not only for their own use. To ensure a harmonised and workable approach across the EU, this and other exemptions should be aligned with established guidance and explicitly confirm that third parties acting on behalf of the controller of the service may benefit from the same exemption. Similarly, the proposed security exemption (see article 88a (3c)) is unduly narrow, as it fails to encompass essential activities such as the detection and prevention of fraud and other illegal activities. The latter positively impact users' experience and safety and are essential safeguards in the provision of digital services and support a vibrant market in the provision of essential services.

The consent exemptions should be extended to cover a broader set of low-impact, essential use cases, in line with a risk-based approach. This is explicitly recommended by the EDPB and EDPS in their joint opinion on the Digital Omnibus. This approach would reduce consent fatigue by removing banners for any service using contextual ads and incentivise privacy-first business models. It would also ensure that regulations align with how digital services operate today, reserving user attention for high-impact personalisation rather than basic operations. This would better reflect what technologies are necessary to operate digital services today, while increasing user recognition of and engagement with genuine personalisation technologies. In the context of online advertising, Article 88a should be amended to include operations that do not involve the tracking of users' activity and are inherently required for the technical delivery and management of advertising campaigns:

- Delivery and display of advertising that does not involve profiling (such as contextual advertising).
- Optimising ad frequency / frequency capping.
- Ensuring security and preventing ad fraud and abuse (e.g. invalid traffic detection, bots identification, domain spoofing, click fraud).
- Verifying and measuring ad delivery (for billing and auditing purposes).

The list should also incorporate use cases that national Data Protection Authorities (DPAs) have already recognised as "strictly necessary" and, as a result, exempted from the consent requirement. These include:

- Providing a consent management platform and storing users' privacy choices[1].
- Storage required to support monetisation models, like metered paywall, cashback, etc.

Beyond advertising-specific use cases, the Article 88a whitelist should also be amended to cover:

- Ephemeral storage (e.g. data temporarily held in memory during web operations such as JavaScript variables, session state, and transient processing data for HTTP requests, which is a technical necessity for basic web functionality) as well as the passive receipt of information communicated as part of the ordinary operation of the internet (e.g., as part of Transmission Control Protocol / Internet Protocol) or the device, provided it is not specifically targeted by the sender or recipient.
- Detection and prevention of fraud, unlawful activities or misuse of the service.
- Software updating/patching and product maintenance.
- A/B testing, product improvement, and user journey optimisation.
- Implementation or Privacy Enhancing Technologies (PETs).

Where these activities are carried out by a third party on behalf of a provider on the provider's service, the third party shall be able to benefit from the same exemption. This streamlined approach would refocus user consent on higher-impact processing where users reasonably expect to have a choice and control under GDPR rules.

2. Renewal of consent (GDPR article 88a (4))

A mandatory six-month consent renewal period would be technically unworkable across different online environments and jeopardise the economic sustainability of media. Imposing a uniform renewal timeline fails to reflect the diversity of digital services, access models, and technical realities across the online ecosystem. For example, in non-authenticated environments, privacy choices are typically 'user-agent'-specific: the same user may access a service via multiple interfaces on the same device, e.g. a native application and a web browser, each maintaining separate and technically independent privacy settings. As a result, a single, fixed renewal period cannot be consistently or reliably implemented across authenticated and unauthenticated services, or across app- and browser-based environments. This complexity is further compounded by user behaviour and browser design choices, as users may delete their privacy preferences from their devices, and certain browsers —

[1] The EDPB and the EDPS also consider an exception to consent for the storing of users' privacy choices should be explicitly added in their joint opinion on the Digital Omnibus.

such as Safari — delete by default first-party cookies, which often store users' privacy choices, seven days after the user's last interaction with the website. Finally, controllers need to renew consent when there is a change of partner.

Recommendation: Given the diversity of data processing activities, online services, and technical environments (app-based vs browser-based; authenticated vs. non-authenticated), the proposed regulation should not impose a rigid consent renewal timeline.

3. Automated user choices and centralised interfaces (GDPR article 88b)

The European Commission has correctly identified the underlying problem: Europe needs a simpler cookie rulebook that reduces consent fatigue. However, the proposal must learn from multiple prior initiatives[2] that demonstrated that browser-based consent mechanisms cannot be operationalised in a manner that is compliant, enforceable, or economically sustainable. By reintroducing this approach through Article 88b, the Commission introduces profound legal and operational uncertainty that risks undermining the provision of ad-funded services.

Cookie fatigue will not be addressed as generic browser-level signals cannot satisfy the GDPR's strict requirements for valid consent. Under Article 4(11) of the GDPR, consent must be "specific," "informed," and "unambiguous." A centralised browser setting operates as a blanket signal, captured before a user interacts with a specific website and understands who is collecting their data or why. This makes it functionally impossible for existing browser-based solutions (e.g. DNT or GPC) to provide the granular detail required to meet the GDPR high standard for "informed" consent.

Centralised consent management is not technically feasible across different online environments and risks undermining user privacy choices. It cannot operate reliably in 'user-centric, multi-terminal consent environments'[3], where online services implement means to persist privacy choices cross-device (e.g. account-based). For example, a user may withdraw consent within a mobile app, but later access the same service through a web browser that continues to signal "consent", as the browser has no technical means to reconcile the updated preference. As a result, this approach does not provide service providers with a legally reliable record of user consent and, rather than strengthening user control over personal data, it may have the opposite effect.

[2] Examples include 2017 ePrivacy Regulation Proposal, 2019 W3C DNT or 2023 Cookie Pledge
[3] See here the CNIL's recommendation on cross-device consent

Decoupling consent from the provider–user relationship risks creating competition challenges and poses a severe economic risk to ad-funded services. A browser-level consent mechanism severs the direct relationship between service providers and users. This prevents providers such as publishers from explaining the specific value exchange that funds free content and services. This is particularly damaging for independent and smaller publishers, as well as competing providers of digital services, who rely on direct engagement with their audiences to sustain their business models. For example, a recent IAB Europe study confirms that consumers are more willing to consent to data collection when they trust and are familiar with the website.

This decoupling is also likely to result in significantly lower consent rates. Users are naturally more conservative when asked to make a single, global choice covering the entire internet than when responding to a request from a specific publisher with whom they have an established relationship. A sharp decline in consent rates would have immediate and substantial economic consequences, most notably reduced advertising revenues for providers of online services and content. This would not only deny access to high-yield ad revenues to fund business investment and growth, but may also result in services exiting the EU market - where they are unable to subsidise large numbers of unconsented users. This would reduce consumer choice over time.

This proposal risks undermining brands' ability - particularly that of SMEs - to measure and optimise advertising spend at a time of significant economic pressure. Digital advertising cannot function effectively without the ability to measure ad campaigns across multiple services. The introduction of centralised privacy controls risks limiting the brands' ability to rely on third-party cookies or equivalent technologies across publishers' websites, disrupting the data flows necessary for effective measurement. Brands would consequently lose the ability to measure the return on their advertising spend, as they would be unable to link ads displayed on publisher sites to purchases on their own websites. This impact is disproportionately severe for smaller brands, which operate with constrained budgets and rely on measurement to optimise advertising spend.

Recommendation:

Article 88b should be deleted, as it revives a repeatedly abandoned concept that is legally flawed, technically unworkable, and economically harmful. Instead, EU policymakers should focus on robust and consistent enforcement of existing GDPR rules and on addressing the root cause of banner proliferation: the excessive reliance on consent as the legal base for all but a few cookie uses without regard to actual risk or

harm (see section above on “Access and storage of personal data in the terminal equipment and subsequent processing”).

4. Media exemption (GDPR article 88b(3))

While we welcome the Commission’s objective to protect media publishers, the proposed exemption - allowing media service providers to ignore browser-level signals - fails to fully achieve the stated objective. Article 88b would allow media service providers to disregard users’ browser-based privacy signals and instead initiate their own consent requests. As currently drafted, the exemption risks undermining the advertising-based business models on which most media publishers depend and falls short of the Commission’s ambition of simplification and legal certainty.

The exemption is structurally misaligned and ignores that media publishers are reliant on a complex supply chain. Media publishers rely on a network of technology partners, including adtech intermediaries acting as data controllers. The current drafting does not recognise this interdependence and assumes that publishers always function in isolation from others.

The exemption is legally uncertain and largely inapplicable to the media supply chain, as it does not clearly extend to adtech intermediaries. Paragraphs 1 and 2 of Article 88b apply to “controllers”, creating significant ambiguity as to whether a media service provider’s partners can also rely on the exemption, such as an adtech intermediary. Given that the majority of media publishers depend on third-party intermediaries to sell and monetise advertising inventory, this uncertainty is not marginal but systemic. If the exemption cannot also apply in these common scenarios, publishers will be unable to monetise their content effectively, despite formally qualifying for the carve-out.

As a result, media publisher inventory will continue to lose value, jeopardising their economic sustainability. When advertisers cannot target or measure campaigns effectively, they will simply pay less for advertising and very much less where users ‘reject all’ cookies and alternative ad models cannot be compliant. This means publisher revenues will decline regardless of the formal existence of an exemption.

The exemption will not necessarily reduce compliance costs and legal uncertainty. The proposed approach will continue to require cookie consent in most cases and will not reduce the cost of implementing and maintaining consent mechanisms for media publishers, whose activities typically extend beyond media services alone. Introducing

different rules for handling user privacy choices under Articles 88a and 88b(3), depending on whether a service qualifies as a media service under the EMFA, fragments compliance obligations and contradicts the Digital Omnibus' objective of simplification. This dual regime would in practice increase technical complexity, heighten legal uncertainty, ultimately raising - rather than lowering - the compliance burden for media providers.

5. Definition of personal data (GDPR article 4 and recital 27)

The amended definition of personal data is a crucial and welcome step towards greater legal certainty. Aligning the GDPR definition of personal data with the CJEU's ruling in EDPS v SRB is a very positive and timely clarification. This amendment confirms that identifiability is contextual, reducing ambiguity, and should strengthen legal certainty for businesses and regulators alike. Importantly, this approach will also incentivise the responsible use of pseudonymisation and anonymisation techniques that can meaningfully reduce or prevent the ability to (re-)identify individuals in practice. Over time, this could support a virtuous circle: encouraging investment in pseudonymisation and anonymisation solutions to facilitate access to data in a way that protects users.

Recital 27 should be further clarified to contribute to a more realistic assessment of identification risk. In line with the CJEU's ruling in Breyer, Recital 27 is particularly helpful in confirming that unlawful means, such as hacking or breaches of contractual obligations, should not be treated as means "reasonably likely to be used" for identification. However, the co-legislators should consider strengthening this recital further to ensure that the concept of "means reasonably likely to be used" is interpreted in a practical manner. This means explicitly excluding purely theoretical or speculative scenarios that are not plausible in real-world conditions, taking into account the technical feasibility and costs of identification. In line with the CJEU's ruling in SRB, this recital should also make clear that the mere ability to single out an individual in a data set does not automatically mean that an individual is identifiable if there are no means to act upon this information in relation to this individual.

6. Re-identification of pseudonymised data (GDPR article 41a)

We strongly welcome the Commission's proposal to use secondary legislation to delineate the boundaries of the GDPR more clearly. IAB Europe supports the

objective of reducing fragmentation and ensuring a more consistent interpretation of the revised definition of personal data across the EU. We consider secondary legislation the most effective tool to achieve this ambition. An implementing act, which would specify means and criteria to assess identifiability risks, will be important. This will provide legal certainty, help organisations of all sizes assess and demonstrate compliance consistently, and ultimately innovate more with enhanced trust.

The co-legislators should broaden the scope of the new article to explicitly cover anonymisation, in addition to pseudonymisation. As currently drafted, pseudonymisation appears to be treated as the sole pathway toward anonymisation. However, anonymisation can also be achieved independently, through technical measures[4] that irreversibly prevent the identification of individuals or only pose minor residual risks. Explicitly extending the provision to anonymisation would better support businesses in assessing identifiability risks when they deploy robust anonymisation techniques, thereby improving legal clarity and predictability. In turn, this would encourage the development and uptake of anonymisation solutions. It is also important to note that pseudonymisation should not only be viewed solely as a transitional step towards anonymisation, but should also be recognised as a standalone privacy-enhancing technique. In practice, it can not only support compliance with key GDPR principles, such as data minimisation, but also lead to the conclusion that the data is no longer non-personal data and as such not subject to the GDPR. This role should be more clearly acknowledged and actively encouraged by European policymakers.

The proposal should better reflect the role of organisational and contractual measures in preventing the re-identification of pseudonymised data. The co-legislators should explicitly recognise privacy-enhancing technologies (PETs) in the "state of the art" assessment, while clarifying that the "means and criteria" used to assess whether pseudonymised data is no longer personal should not be limited to such measures. While technical safeguards are essential, effective risk mitigation also depends on organisational and contractual measures that prevent re-identification. These include contractual restrictions prohibiting recipients from re-identifying individuals or sharing data onward. Recognising the combined role of technical, organisational, and contractual safeguards would better align the legal assessment with operational realities, and ultimately incentivise responsible data sharing practices while protecting user privacy.

[4] Examples of such technical measures include k-anonymity or aggregation.

Observations and recommendations on other issues

Issue	Observations	IAB Europe's recommendations
Prohibition on the processing of special category data GDPR Article 9	• We welcome the new provisions on special categories usage (articles 9 (2)(k) & 9 (5)), which bring more context to how sensitive attributes can be processed in the development, testing and operation of AI systems. They recognise that, in some circumstances, exposure to special categories is unavoidable and can be done under strict safeguards, which align very closely to those recommended in the CNIL's guidance on sensitive data processing in an AI context. • However, the proposed exemption relies on strict filtering obligations—requiring developers to scrub training datasets and implement output filters to prevent disclosure of Special Category of Data (SCD). This creates a paradox: to detect SCD, controllers will have to proactively process	The co-legislators should refine these safeguards to ensure they do not unintentionally break the utility of Generative AI or hinder bias mitigation efforts. The focus should be on "appropriate safeguards" (such as adversarial testing and PETs) rather than rigid filtering mandates that may contradict the functional design of AI products.

	additional SCD, increasing the risks for users' privacy. Strict output filters could also degrade the utility of Generative AI products designed to provide descriptive, factual information about the world.	
Data protection impact assessment GDPR Article 35	<u>List of processing operations subject to DPIA</u>: ● The proposal to harmonise the list of processing operations requiring a DPIA via a central EU mechanism is a positive step. This standardisation has the potential to significantly reduce compliance costs and complexity for pan-European companies. ● However, there is a risk that the new EDPB list could diverge significantly from the existing lists established by national supervisory authorities. If the EDPB amalgamates all national requirements into a "super-list," it would create a far more onerous burden than currently exists. Furthermore, the proposal fails to clarify how new lists apply to existing products. It is logically impossible to conduct a DPIA "prior to processing" (as required by Art. 35) for	We recommend that the text explicitly states that new DPIA provisions only apply to new processing operations. Existing processing, which is already compliant under current national guidance, should not be subject to retroactive assessments. <u>List of processing operations subject to DPIA</u>: Co-legislators should ensure that the EDPB's harmonised list reflects the existing consensus of national supervisory authorities rather than creating new, expansive guidance. <u>Common template and methodology for conducting DPIA:</u> While welcoming guidance on DPIA templates and methodologies, we caution for mandatory models,

	operations that have been running safely for years. Without a clear “grandfather clause,” businesses face legal limbo regarding established services, risking retroactive non-compliance.	which risk adding new costs for controllers to adapt their frameworks and would reduce their ability to adapt DPIAs to the specific aspects of processing.

Annex:

Challenges posed by Centralised Consent Management

Executive summary

IAB Europe shares the Commission's ambition to reduce consent fatigue. However, we maintain that a centralized, browser-based consent management system is not a viable solution for this issue, as it is not legally and technically feasible across different online environments.

First, browser-based consent choices cannot satisfy the GDPR's requirements for informed and specific consent. In order to consent, users must be informed of the purposes of processing, the identity of the controller(s), the categories of data collected, retention periods, etc. - all of which can vary substantially from one website to another. Moreover, the specific purposes of processing cannot be anticipated and pre-defined within a generic browser-level consent mechanism, which would effectively prevent any innovation in data processing approaches.

Second, browser-based consent management cannot operate reliably in cross-device environments, creating signalling conflicts that undermine both user consent choices and legal compliance for Controllers who could be left with an unreliable record of user consent.

First challenge: Information and consent choices are service-specific

From one online service to another, the purposes for which consent is sought vary materially as each online service publisher operates a distinct service model and corresponding data processing. In the Open Web in particular, many publishers do not operate proprietary technologies for measuring their audience, selling ad placements, or personalising content, but rely on a range of third-party companies to perform these operations. Only the publisher has access to the detailed information necessary to build the relevant consent interfaces that accurately reflect its particular data processing activities and present meaningful choices to the end-user (e.g. identity of third-party companies susceptible to collect data, the purposes pursued, the data retention periods, etc.).

These elements are central to the transparency and specificity requirements applicable to valid consent and cannot be meaningfully standardised independently of the service context.

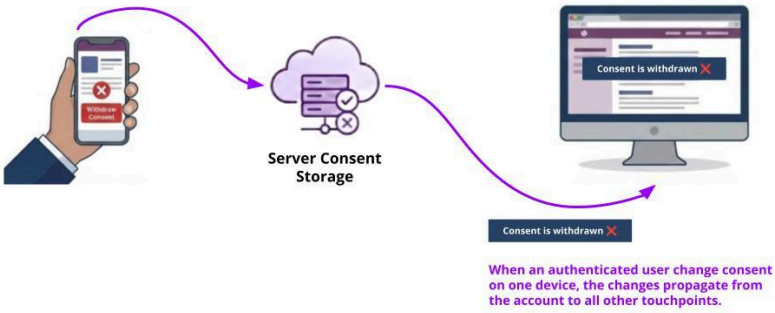
Moreover, the assessment of whether consent is informed, specific, and freely given is closely linked to the reasonable expectations of users in light of the nature of the service. For example, an online service that is offered without direct monetary payment and financed through advertising may seek consent for purposes relating to the delivery of advertising. In such a context, users may reasonably understand that advertising-related processing forms part of the economic model of the service, which is relevant when assessing user expectations and the validity of consent. By contrast, a service whose core function is to enable individuals to complete tax filings or access essential administrative or compliance-related functions typically does not rely on advertising-based monetisation. In that context, requests for consent for purposes relating to advertising would fall outside users' ordinary expectations associated with the service.

This service-specific nature of consent requirements makes centralised, browser-level consent management legally and technically inadequate, as it cannot account for the nuanced and varied consent scenarios that exist across different online services.

Second challenge: authenticated environments can store privacy preferences

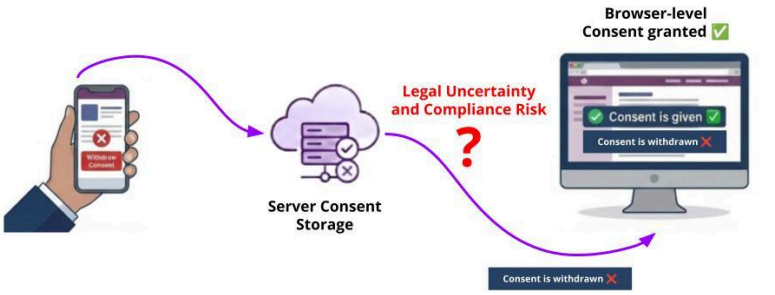
Authenticated environments enable user-centric consent choices through:

- Cross-device consent persistence.
- Reduced consent fatigue through unified settings that eliminate the need for users to repeatedly configure the same privacy preferences across different access methods or devices (mobile app, web browser, tablet, etc.).
- Technical capability to maintain privacy preferences across all access points so that they are preserved and applied consistently.



On the opposite side, article 88(b)(6)[5] is technically unworkable because browser-level consent choices (where consent choices are stored locally by a browser without user authentication) cannot function effectively in cross-device consent environments (where users log into services and expect their privacy preferences to follow them across devices). A similar approach would create critical signalling conflicts, as shown in the scenario below:

1. User withdraws consent within a mobile app (authenticated environment).
2. User later accesses the same service through a web browser.
3. Browser continues to signal "consent" because it has no technical means to reconcile the updated preference.
4. Online service receives conflicting signals about the same user's consent choices.



5. The service provider now holds two different consent choices for the same user: one device-based record indicating "Consent Withdrawn" (from the mobile app) and one browser-based record indicating "Consent Granted" (from the web browser). This creates a conflicting compliance situation about which record should be legally recognised.

---

[5] *Providers of web browsers, which are not SMEs, shall provide the technical means to allow data subjects to give their consent and to refuse a request for consent and exercise the right to object pursuant to Article 21(2) through the automated and machine-readable means referred to in paragraph 1 of this Article, as applied pursuant to paragraphs 2 to 5 of this Article.*

This scenario demonstrates how centralised, browser-level consent management can create legal uncertainty for controllers and confuse users, as it is susceptible to undermining the persistence of their privacy preferences across multiple access points.